

Security for peer networks

Peer-to-Peer (P2P) is a popular concept. Networks like BitTorrent and eMule make it easier for people to share data.

Peer-to-Peer (P2P) is a popular concept. Networks like BitTorrent and eMule make it easier for people to share data. If I have something you need and you have something I want then why can't we share it with each other? For one thing, shared files on your computer for unknown users on the public Internet can put your computer at risk for safety and security. So keep in mind that your computer must have a firewall, you can use the built-in firewall on your router or a personal firewall software such as **ZoneAlarm**.

However, to share files on your computer and sometimes to be able to open files on another computer via a peer-to-peer network like BitTorrent, you must open a special port on the firewall so that P2P software can transmit. believe. In fact, when you open a port on the firewall, there will be many dangers from malicious attacks on the computer through that open port.



Another security concern is that when you download files from peer networks like BitTorrent, eMule or other networks, you are not sure if the file is dangerous. You think you have downloaded a great utility, but when you double-click on the EXE file, is there any guarantee that you are not activating the Trojan or backdoor installation on your own computer? And through that, the attacker can access your computer easily.

Therefore, take note of the following 4 key points to consider using peer-to-peer networks as safely as possible:

1. Do not use P2P in the corporate network

At least do not install or use peer networks to share data in the corporate network without explicit permission. Many peer users download files from your computer will slow down network bandwidth. But that is only the best situation. Maybe you could unfortunately share sensitive and confidential documents of the company, and that's the worst scenario.

2. Be cautious with workstation software

There are two reasons you should be cautious with peer-to-peer software that software is constantly being developed and it may contain malicious code. Installing the software may be the cause of an error with your computer system. Another factor is that client software is usually stored on multiple computers and may be replaced by malicious versions, which will install viruses or Trojans on your computer once you download them. Peer-to-data file sharing users must have at least one security software installed on the device to ensure that malicious code is not easily compromised and replaces the original file share.

3. Don't share everything



When you install P2P client software and access a peer-to-peer network like BitTorrent, there is usually a default folder specified for sharing during the installation process. The specified directory will contain only the files you want to share with all users in the P2P network. Many users unknowingly specify the root ' C: ' as the folder containing the shared file; Allows anyone in the peer network to view and access virtual files or folders in that drive - including system files.

4. Scan everything before using

You should carefully review all downloaded files to your computer with maximum alertness. As mentioned above, there is almost no way to ensure that the downloaded file does not contain Trojans or viruses. It is very

important that you always run 24-hour computer protection software (eg **Prevx Edge** software). You should also regularly scan your computer using the dedicated **Ad-Aware** tool to make sure you don't install the wrong spyware on the system. In addition, you must perform an antivirus program update regularly to ensure that you always deal with the latest viruses and scan any downloaded files before opening them.

Scanning all files before opening them will help you to avoid the most dangerous threats, but not completely avoided. Please collect yourself the necessary knowledge to ensure your computer when accessing the network still ensures safety and security.

You finished reading the article "**Security for peer networks**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.